Course Notes for Math 737 (Algebraic Geometry)

3. Hilbert Bases and Polynomials. Two important theorems of Hilbert are proved, and some consequences are investigated.

Recall that in §2, we observed:

$$V(\{L_s\}_{s\in S}) = V(L_{s_1}, ..., L_{s_r}) \subset \mathbf{P}(V)$$

for linear forms L_s and suitable (finite!) choice of $s_1, ..., s_r$. Our first task is to generalize this finiteness to all algebraic sets.

Lemma 3.1: Suppose that $f_s, g_t \in k[x_1, ..., x_n]$ for each $s \in S$ and $t \in T$. Let I be the ideal generated by $\{f_s\}_{s\in S}$ and J be the ideal generated by $\{g_t\}_{t\in T}$. Then:

$$J \subseteq I \Rightarrow V(\{f_s\}_{s\in S}) \subseteq V(\{g_t\}_{t\in T}) \subseteq \mathbf{A}_k^n.$$

Proof: Any $g_t \in J \subset I$, so by definition, there are polynomials $f_{s_1}, ..., f_{s_r}$ and $h_1, ..., h_r \in k[x_1, ..., x_n]$ such that

$$g_t = h_1 f_{s_1} + ... + h_r f_{s_r}$$

If $p \in V(\{f_s\}_{s\in S})$ then $f_s(p) = 0$ for all $s \in S$, so by the sum above, $g_t(p) = 0$ for all $t \in T$. Thus $V(\{f_s\}_{s\in S}) \subseteq V(\{g_t\}_{t\in T})$.

Note: In particular, applying the Lemma twice gives us:

$$I = J \Rightarrow V(\{f_s\}_{s\in S}) = V(\{g_t\}_{t\in T})$$

so that we can really think of V as a function from the **ideals** in $k[x_1, ..., x_n]$ to algebraic subsets of $\mathbf{A}_k^n$ (and similarly in the projective case). Note that the reverse implication is often false(!)

Definition: A commutative ring A with 1 is **Noetherian** if every ascending chain of ideals in A:

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq ...$$

stabilizes (i.e. if there is an r such that $I_r = I_{r+1} = ...$).

Examples: (a) Any ring with finitely many ideals, e.g. a field, is Noetherian.

(b) $\mathbf{Z}$ is Noetherian. Every ideal is of the form $n\mathbf{Z}$ for some $n \in \mathbf{Z}$, and $n\mathbf{Z} \subseteq m\mathbf{Z}$ iff $m|n$, so in particular, $n\mathbf{Z} \subseteq m\mathbf{Z}$ implies $|m| \leq |n|$.

(c) A polynomial ring $k[x_1, x_2, ...,]$ in infinitely many variables is not Noetherian. The chain of ideals: $\langle x_1 \rangle \subset \langle x_1, x_2 \rangle \subset ...$ does not stabilize.

Lemma 3.2: A is Noetherian iff every ideal $I \subset A$ is finitely generated.

Proof: Suppose that every ideal is finitely generated. If $I_1 \subseteq I_2 \subseteq ...$ is an ascending chain of ideals in A, let $I = \cup_{j=1}^{\infty} I_j$. Then I is an ideal, which must be finitely generated by assumption. But the generators must all appear in some I_r (why?) which implies $I = I_r = I_{r+1} = ...$

On the other hand, suppose that $I \subset A$ is not finitely generated. Then we can inductively choose elements $a_1, a_2, ... \in I$ so that $a_{r+1} \notin \langle a_1, ..., a_r \rangle$ for all r. These ideals generated by $a_1, ..., a_r$ form an ascending chain which does not stabilize.

Hilbert Basis Theorem: If A is Noetherian, then $A[x]$ is Noetherian.

Proof: Suppose $I \subset A[x]$ is an ideal. Consider the following ideals in A:

$$J_d := \{a \in A | \ \exists f(x) \in I \text{ of the form } f(x) = ax^d + \ \{\text{lower order in } x\}\}.$$

Then the ideals J_d form an ascending chain, so since A is Noetherian, there must be an r such that $J_r = J_{r+1} = ...$

Each J_d is finitely generated, since A is Noetherian, say by elements $a_{d,i}, i = 1, ..., n_i$. For all d from 1 to r and generators $a_{d,i}, i = 1, ..., n_i$, let $f_{d,i} \in I$ be polynomials of degree d with leading term $a_{d,i}$. Then because of the fact that the chain of ideals stabilizes at J_r, given any polynomial $f \in I$, we can match its leading coefficient *and degree* with a polynomial in the ideal spanned by the $f_{d,i}$, so by induction on the degree of f, we find that the finite collection of polynomials $f_{d,i}$ generate I, which proves $A[x]$ is Noetherian.

Now we are ready for the:

Corollary 3.3: If $V(\{f_s\}_{s \in S}) \subseteq \mathbf{A}_k^n$ is an algebraic subset, then there are finitely many elements $s_1, ..., s_r \in S$ so that:

$$V(\{f_s\}_{s \in S}) = V(f_{s_1}, ..., f_{s_r})$$

Proof: By the note following Lemma 3.1, it suffices to show that the ideal generated by the f_s can be generated by finitely many of them. By the Basis Theorem and induction, the ring $k[x_1, ..., x_n]$ is Noetherian.

Thus at least we know that the ideal generated by the f_s is finitely generated. But in addition, if the inclusions of ideals $\langle f_{s_1}, ..., f_{s_r}\rangle \subset \langle \{f_s\}_{s\in S}\rangle$ were proper for all r, then we could find elements $s_1, s_2, ... \in S$ such that $f_{s_{r+1}} \notin \langle f_{s_1}, ..., f_{s_r}\rangle$ for all r. As in the proof of Lemma 3.2, the chain of ideals generated by $f_{s_1}, ..., f_{s_r}$ would not stabilize, violating the Noetherian property. The upshot of this is that not only is the ideal generated by the f_s finitely generated, but a finite set of generators may be chosen from among the f_s themselves.

Remark: The same proof gives the same result for algebraic subsets of projective space, too.

The next goal of this section is to find a polynomial attached to each projective variety. This will follow from some general results on graded modules over a polynomial ring which we list below.

Let $A = k[x_0, ..., x_n]$ be the polynomial ring graded by degree.

Definitions: (a) A **graded A-module** M is a module over A together with a decomposition (as a vector space over k) as:

$$M = \bigoplus_{d\in\mathbf{Z}} M_d$$

with the property that if $f \in A_d$ and $m \in M_e$ then $fm \in M_{d+e}$. Notice that in contrast to graded rings, we allow summands indexed by negative integers.

(b) An A-module homomorphism $\alpha : M \to N$ is a homomorphism of graded modules if M and N are graded and $\alpha(M_d) \subset N_d$ for all $d \in \mathbf{Z}$.

(c) If M is a graded A-module and $p \in \mathbf{Z}$, define the **twist** $M(p)$ to be the graded A-module defined by $M(p)_d = M_{d+p}$. (This operation is invertible!) For instance, multiplication by a homogeneous polynomial $F \in A_e$ determines graded homomorphisms $m_F : M(p) \to M(p+e)$ for all twists p.

(d) If M is a graded A-module and all the M_d are finite-dimensional vector spaces, the associated **Hilbert function** is:

$$h_M : \mathbf{Z} \to \mathbf{Z}_{\geq 0};\quad d \mapsto \dim_k M_d$$

Examples: (a) A itself with its grading is a graded A-module. Its Hilbert function is:

$$h_A(d) = \begin{cases} \binom{n+d}{n} = \frac{(n+d)(n+d-1)...(d+1)}{n!} \text{ if } d \geq 0 \text{ and} \\ \\ 0 \text{ if } d < 0 \end{cases}$$

Notice that $\binom{n+d}{n}$ is polynomial of degree n in d with leading term $\frac{1}{n!}d^n$.

(b) Let $I \subset A$ be a homogeneous ideal. We will be particularly interested in the Hilbert function of A/I (thought of as a graded A- module). We can compute some special cases:

(b1) Suppose $F \in A$ is homogeneous of degree e and $I = \langle F \rangle$. Then $I \cong A(-e)$ as graded A-modules(!) so that:

$$h_{A/I}(d) = h_A(d) - h_I(d) = h_A(d) - h_A(d-e)$$

and we get the following Hilbert function for A/I:

$$h_{A/I}(d) = \begin{cases} 0 \text{ if } d < 0 \\ \\ \binom{n+d}{n} \text{ if } 0 \leq d < e \text{ and} \\ \\ \binom{n+d}{n} - \binom{n+d-e}{n} \text{ if } d \geq e \end{cases}$$

Notice that $h_{A/I}(d)$ is a polynomial in d with leading term $\frac{e}{(n-1)!}d^{n-1}$ as soon as $d \geq e$.

(b2) Let k be an infinite field, let $Z \subset \mathbf{P}^n_k$ be a set consisting of m points, and let $I = I(Z) \subset A$ be the homogeneous geometric ideal defined by Z. Then I claim the following:

Lemma: $h_{A/I}(d) = m$ for all $d \geq m-1$.

Proof: Recall from §2 that we can think of the inclusion of a point $p \hookrightarrow \mathbf{P}^n_k = \mathbf{P}(V)$ as ι_W where $W \subset V$ is a line through the origin. Let e_p be a nonzero vector in W, and y_p the dual vector. Then we have the corresponding $\iota_W^* : k[x_0, ..., x_n]_d \to k[y_p]_d \cong k$ for each $p \in Z$, which is surjective for each p individually. Moreover, I_d is the kernel of the map:

$$\rho_d : k[x_0, ..., x_n]_d \to k^m \cong \bigoplus_{p \in Z} k[y_p]_d$$

Thus, we need to prove that ρ_d is surjective if $d \geq m-1$. But consider the set $Z - \{p\}$. This is algebraic because it is finite (§1 HW) and moreover, you discovered that $Z - \{p\} = V(J)$ where J is generated by homogeneous polynomials of degree $m-1$. But this implies that we can find homogeneous polynomials of degree $m-1$ (and any larger degree..why?) which vanish at all the points of Z except for p. Such polynomials are mapped to a basis for k^m by ρ_d, hence surjectivity.

Exercise: (a) Find the natural grading on the cokernel and kernel of a graded homomorphism of graded A-modules.

(b) Prove that if

$$0 \to M^1 \to ... \to M^r \to 0$$

is a long exact sequence of graded homomorphisms of graded A-modules with Hilbert functions $h_{M^i}(d)$, then $\sum_{i=1}^r (-1)^i h_{M^i}(d)$ is the zero function.

(c) If M is a finitely generated graded A-module, prove that $M_d = 0$ for $d << 0$ and that the vector spaces M_d are all finite dimensional. Thus finitely generated graded A-modules always have Hilbert functions.

(d) If $\alpha : M \to N$ is a homomorphism (not necessarily graded!) of finitely generated A-modules, prove that the kernel and cokernel of α are also finitely generated. (Hint: A is Noetherian!)

Definition: If M is a graded A-module with Hilbert function $h_M(d)$, then the "Laurent series":

$$P_M(t) := \sum_{d \in \mathbf{Z}} h_M(d) t^d \in \mathbf{Z}[[t^{-1}, t]]$$

is called the **Poincaré series** of M.

Note that if M is finitely generated, then by Exercise (c) above, the Poincaré series is bounded from below (i.e. $P_M(t) = a_{-k}t^{-k} + a_{-k+1}t^{-k+1} + ...$), but that it is usually not bounded from above. If it were, then $P_M(t)$ would be a Laurent **polynomial**, that is, an element of $\mathbf{Z}[t^{-1}, t]$.

More Observations: (1) Given an exact sequence of graded A-modules as in Exercise (b) above, then $\sum_{i=1}^r (-1)^i P_{M^i}(t) \equiv 0$.

(2) For any twist, $P_{M(p)}(t) = t^{-p} P_M(t)$.

Hilbert's Polynomial Theorem (with contributions by Serre):

If M is a finitely generated graded $k[x_0, ..., x_n]$-module, then:

(a) $(1-t)^{n+1}P_M(t) \in \mathbf{Z}[t^{-1}, t]$.

(b) There is a (uniquely determined) polynomial $H_M(x) \in \mathbf{Q}[x]$ such that $H_M(d) = h_M(d)$ for all sufficiently large d. Moreover, if $H_M(d) \not\equiv 0$, let $d_M =$ deg$(H_M(d))$. Then

$$f(t) := (1-t)^{d_M+1}P_M(t) \in \mathbf{Z}[t^{-1}, t] \text{ and } f(1) \neq 0$$

(so that in particular, $d_M \leq n$.)

Proof: We prove (a) by induction on the number of variables. If $n = -1$, then M is a finite dimensional vector space over k, hence $M_d = 0$ for d sufficiently large and sufficiently small, so $P_M(t) \in \mathbf{Z}[t^{-1}, t]$ which is (a).

Next, suppose $n \geq 0$ and consider the exact sequence:

$$(*) : \quad 0 \to K \to M \stackrel{x_n}{\to} M(1) \to N \to 0$$

where K and N are the kernel and cokernel of the graded homomorphism given by multiplication by x_n. Notice that K and N are graded finitely generated modules over the ring $k[x_0, ..., x_n]/(x_n) \cong k[x_0, ..., x_{n-1}]$, so we are in a position to prove (a) by induction. Namely, by Observations (1) and (2), we have:

$$(t^{-1} - 1)P_M(t) = P_{M(1)}(t) - P_M(t) = P_N(t) - P_K(t)$$

so that $(1-t)^{n+1}P_M(t) = t(1-t)^n(P_N(t) - P_K(t)) \in \mathbf{Z}[t^{-1}, t]$.

To prove (b), we calculate. First, let $P_M(t) = (1-t)^{-p}g(t)$ such that g has neither a zero nor pole at 1. We want to show $h_M(d)$ is a polynomial of degree $p-1$ in d for large d. But

$$(1-t)^{-p} = \sum_{r=0}^{\infty} \binom{p+r-1}{p-1} t^r$$

and if we let $g(t) = \sum_{k=-N}^{N} a_k t^k$, then for large enough d, we have:

$$h_M(d) = \sum_{k=-N}^{N} a_k \binom{p+d-k-1}{p-1}$$

But this is a polynomial of the form:

$$\frac{g(1)}{(p-1)!}d^{p-1} + \text{ lower order terms}$$

Since $g(1) \neq 0$ by assumption, this completes the proof of (b), hence of the Polynomial Theorem.

Definition: The polynomial $H_M(d)$ associated to a finitely generated graded A-module M is called the **Hilbert polynomial** of M.

We'll give another proof of the fact that $h_M(d)$ is a polynomial for $d >> 0$, partly as an excuse for introducing the following important basis for the **Z**-module consisting of all integer-valued polynomials:

$$H : \mathbf{Z} \to \mathbf{Z}$$

Lemma 3.4: If $H : \mathbf{Z} \to \mathbf{Z}$ is a polynomial of degree p (in $\mathbf{Q}[x]$), then :

$$H(d) = a_0 \binom{d}{p} + a_1 \binom{d}{p-1} + ... + a_{p-1} \binom{d}{1} + a_p$$

where the $a_i \in \mathbf{Z}$ are uniquely determined. Moreover,

$$H(d+1) - H(d) = a_0 \binom{d}{p-1} + a_1 \binom{d}{p-2} + ... + a_{p-1}.$$

Proof: The $\binom{d}{p-i}$ are of different degrees, hence linearly independent. This proves uniqueness of the a_i. One computes the a_i by evaluating $H(d)$ at $d = 0, 1, ..., p$ (that's $p+1$ points!). The last statement is an identity of binomial coefficients, which is easily checked.

Alternate proof that h_M is a polynomial in large degrees: Using the exact sequence $(*)$ and induction on the number of variables again, we see that

$$h_M(d+1) - h_M(d) = H_K(d) - H_N(d)$$

for all sufficiently large d. If we let $p =$ deg$(H_K - H_N)$, then from Lemma 3.4, we can find a polynomial H_M of degree $p+1$ which has has the property that for **all** d,

$$H_M(d+1) - H_M(d) = H_K(d) - H_N(d)$$

Moreover, all the coefficients of H_M are determined (in the canonical expansion of the Lemma) except for the constant term, which we set so that $H_M(d) = h_M(d)$ for some (large!) d. Then $h_M(d) = H_M(d)$ for all sufficiently large d, as desired.

Definition: If $X \subset \mathbf{P}_k^n$ is a projective variety, then the **Hilbert polynomial of** X is by definition the Hilbert polynomial of $k[X]$ as a $k[x_0, ..., x_n]$-module.

Some Motivation: A lot of geometric information about $X \subset \mathbf{P}_k^n$ is encoded in its Hilbert polynomial. For example, we will eventually prove that if k is algebraically closed and

$$H_X(d) = \frac{a_m}{m!} d^m + \text{ lower order (where } a_m \neq 0\text{), then:}$$

(i) m is equal to the dimension of X, and

(ii) a "general" projective subspace $\Lambda \subset \mathbf{P}_k^n$ of **codimension** m intersects X in exactly a_m points (we will call this the **degree** of X).

Here is another observation about the Hilbert polynomial:

Lemma 3.5: Let M be a finitely generated graded A-module and suppose that $F \in A_e$ has the property that $0 \in M$ is the only element annihilated by F. Let $N = M/FM$. Then:

$$\deg(H_N) = \deg(H_M) - 1$$

and if $H_M(d) = \frac{a_0}{m!} d^m +$ lower order, then $H_N = \frac{e a_0}{(m-1)!} d^{m-1} +$ lower order.

Proof: Since F only annihilates 0, the map $M(-e) \to M$ given by multiplication by F is injective. Thus, from the exact sequence of graded A-modules:

$$0 \to M(-e) \stackrel{m_F}{\to} M \to N \to 0$$

we see that $H_N(d) = H_M(d) - H_M(d-e)$, which is a polynomial of degree exactly $\deg(H_M) - 1$. The leading term is computed by applying Lemma 3.4 to the telescoping sum:

$$H_M(d) - H_M(d-e) = (H_M(d) - H_M(d-1)) + (H_M(d-1) - H_M(d-2)) + ...$$

Definition: (a) An ideal $I \subset A$ is called a **complete intersection ideal** if there are generators $F_1, ..., F_r \in I$ with the property that each F_i is not a zero divisor in $A/\langle F_1, ..., F_{i-1}\rangle$.

(b) A variety $X \subset \mathbf{A}_k^n$ is called a **complete intersection** if $I(X)$ is a complete intersection ideal.

(c) A variety $X \subset \mathbf{P}_k^n$ is called a **complete intersection** if $I(X)$ can be generated by **homogeneous** elements as in (a).

Observation: If $X \subset \mathbf{P}_k^n$ is a **complete intersection**, with generators F_i of degree d_i satisfying (a), then the Hilbert polynomial of X is of the form:

$$H_X(d) = \frac{d_1 \cdots d_r}{(n-r)!} d^{n-r} + \text{ lower order terms}$$

Proof: Repeated use of Lemma 3.5.

Third Homework Assignment

1. On the function V from ideals in $k[x_1, ..., x_n]$ to algebraic subsets of $\mathbf{A}_k^n$:

(a) Show that $V(I) \cup V(J) = V(IJ)$ (where IJ is the product of ideals).

(b) Show that $\cap_{s \in S} V(I_s) = V(\sum_{s \in S} I_s)$.

(c) Find an infinite union of algebraic subsets which is not algebraic.

2. More on V and I:

(a) If $X \subset \mathbf{A}_k^n$ is an algebraic subset, prove that $V(I(X)) = X$.

(b) If $I \subset k[x_1, ..., x_n]$ is a geometric ideal, prove that $I(V(I)) = I$.

(c) Prove Craw's converse to Lemma 1.1. Namely, if V is an algebraic set and $I = I(V)$ is a prime (geometric) ideal, then V is irreducible.

3. Prove the exercises preceding the Polynomial Theorem.

4. Let's compute some Hilbert functions:

(a) Suppose that $m \leq n$ and $p_1, ..., p_m \in \mathbf{P}_k^n$ span a projective subspace of dimension $m - 1$ (the maximum possible!). Let $Z = \{p_1, ..., p_m\}$ and let $I = I(Z)$. Prove that $h_{A/I}(0) = 1$ and $h_{A/I}(d) = m$ for all $d > 0$. In other words, we match the Hilbert polynomial starting from degree 1.

(b) At the other extreme, suppose $p_1, ..., p_m \in \mathbf{P}_k^n$ are distinct (no condition on m) and only span a projective **line**. Prove that $h_{A/I}(d)$ does not match the Hilbert polynomial until $d = m - 1$. In fact, write down the Hilbert function of A/I(!)

5. The **twisted cubic** and **rational normal curves**: let $\iota_3 : \mathbf{P}_k^1 \to \mathbf{P}_k^3$ be defined by $\iota_3(s : t) = (s^3 : s^2t : st^2 : t^3)$ together with compatible map $\iota_3^* : k[x_0, x_1, x_2, x_3] \to k[s, t]$. The image, which we'll denote by C, is called the **twisted cubic**. Assume k is infinite, and let $I = I(C)$.

(a) Find I_2 explicitly. Prove that C is a variety of dimension 1.

(b) Calculate the Hilbert function of C.

(c) Prove that $I(C)$ is not a complete intersection ideal.

(d) Do (a)-(c) for $\iota_d : \mathbf{P}_k^1 \to \mathbf{P}_k^d$ given by $\iota_d(s : t) = (s^d : s^{d-1}t : ... : t^d)$, and the image, (in case $d \geq 3$) which is called the **rational normal curve**.